Welcome to our webinar

Today this webcast is brought to you by Avanade.

We will begin soon

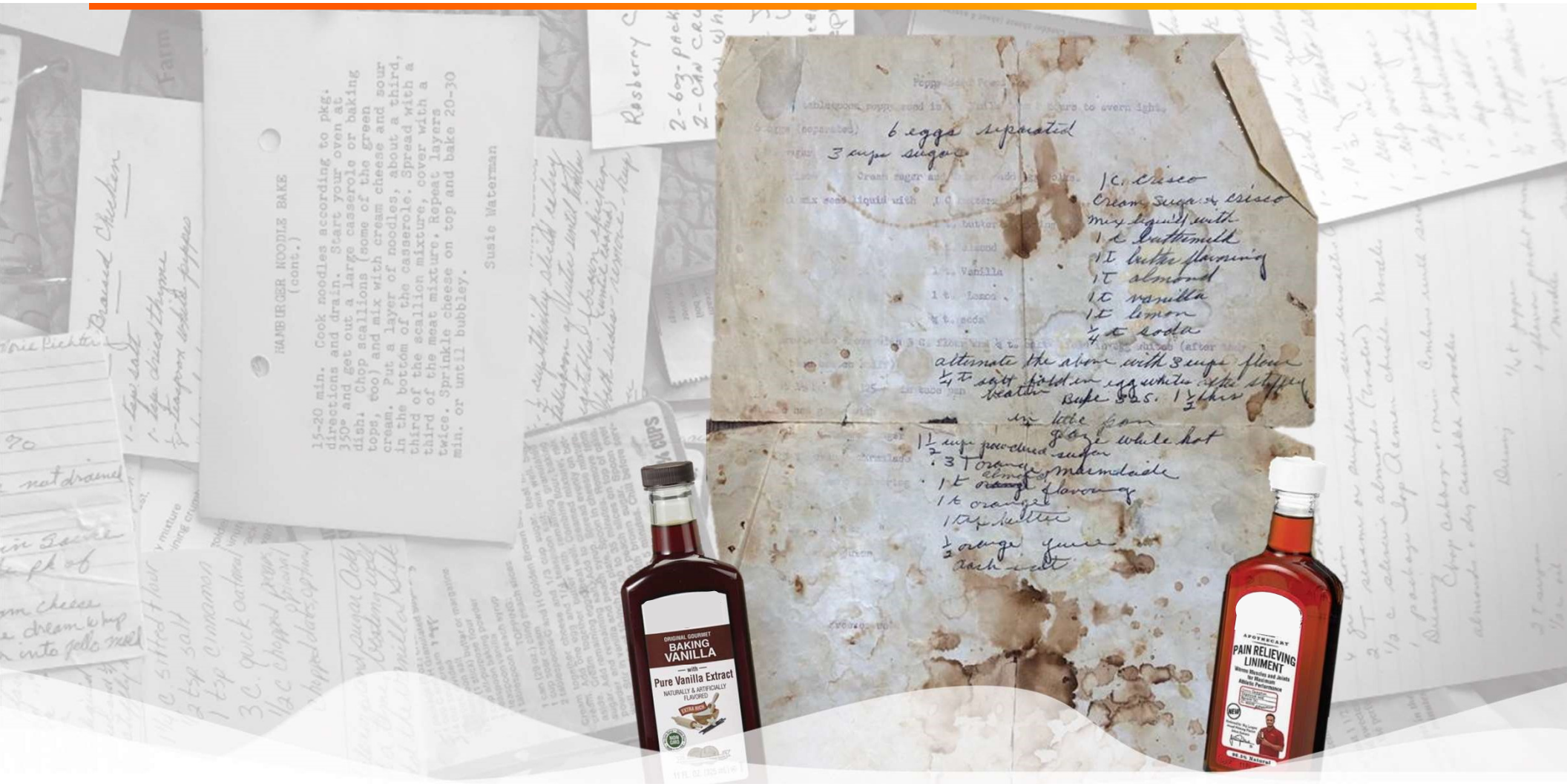
avanade

"Recipes" to start your **Zero Trust journey**

Sue Bohn, (aka Sue Chef)
Partner Director,
Microsoft Identity

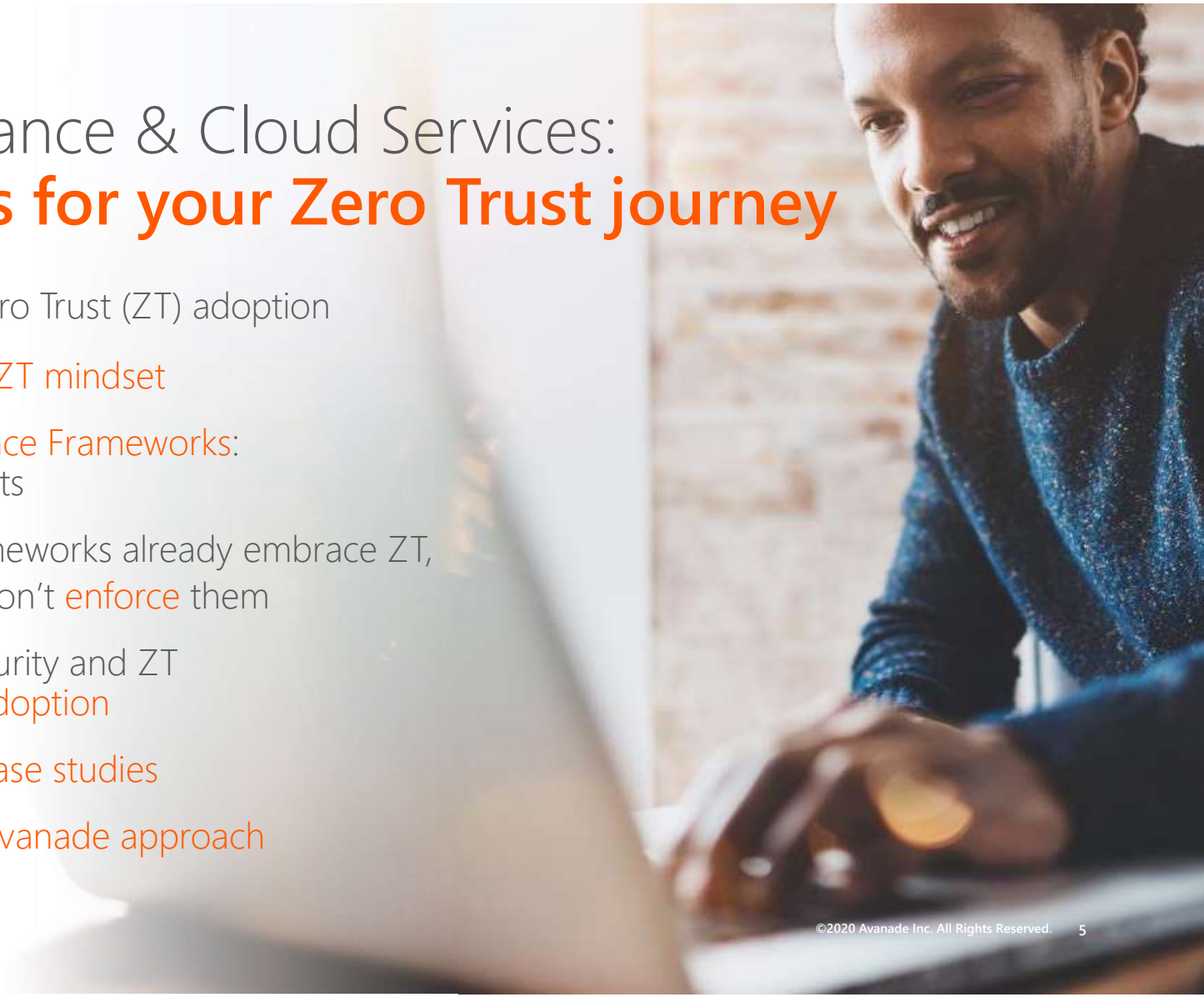
Chris Richter,
Security Practice Leader
Avanade

avanade Microsoft



avanade Microsoft

Security Governance & Cloud Services:
Key ingredients for your Zero Trust journey



- Issues & trends driving Zero Trust (ZT) adoption
- Why we must embrace a ZT mindset
- ZT and Security Governance Frameworks: complementary ingredients
- Security Governance Frameworks already embrace ZT, but many organizations don't enforce them
- Accelerating Security maturity and ZT through Cloud Services adoption
- Partial Trust vs. ZT: Four case studies
- Beginning the journey - Avanade approach

avanade Microsoft

Issues & trends driving **Zero Trust adoption**

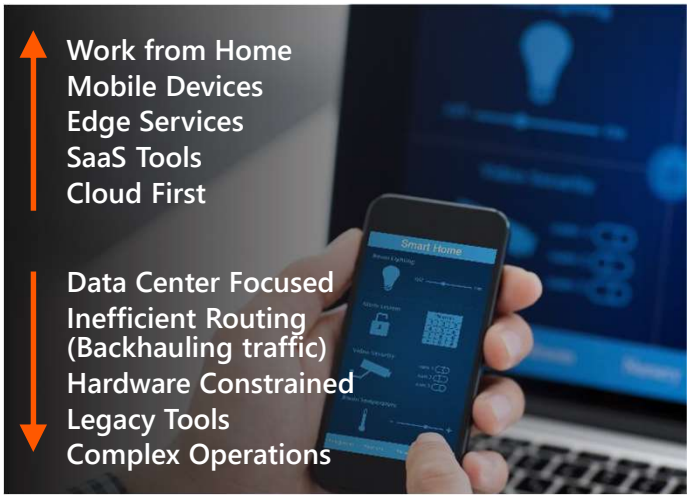
Do you have a strategy for protecting and managing sensitive and business critical data across your organization?

Do you know where your business critical and sensitive data resides and what is being done with it?

Do you have control of data as it travels inside and outside of your organization?

Are you using a solution to classify, label, and protect data?

How can you assess your current compliance posture against exponential data growth and the latest regulations?



>55%

of corporate data is "dark" – it's not classified, protected or governed[2]

#1

Protecting and governing sensitive data is biggest concern in complying with regulations[2]

88%

of organizations no longer have confidence to detect and prevent loss of sensitive data[1]

65%

of leaders agree that moving from hierarchical to team based working is critical for success, but only 7% are ready

avanade Microsoft

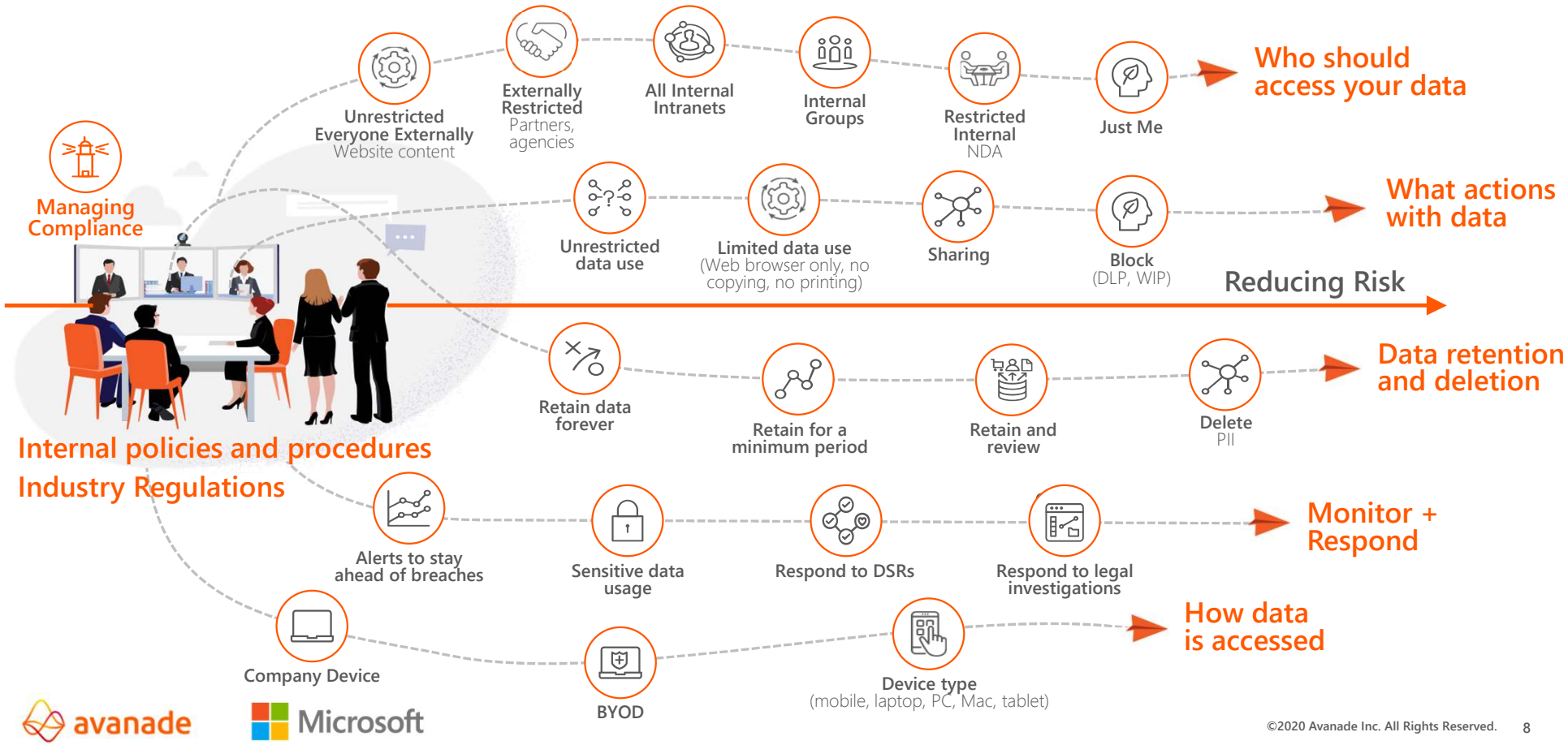
1. Forrester. Security Concerns, Approaches and Technology Adoption. December 2018
2. Microsoft GDPR research, 2017

Old World vs. New World

Users are employees		Employees, partners, customers, bots
Corporate managed devices		Bring your own devices and IoT
On-premises apps		Explosion of cloud apps
Monolithic apps		Composite apps & public restful APIs
Corp network and firewall		Expanding perimeters
Local packet tracking and logs		Explosion of signal

avanade Microsoft

Why we must embrace a **Zero Trust mindset**



avanade Microsoft

Zero Trust Architectures (ZTA) and Security Governance Frameworks: **Complementary ingredients**

Governance, Risk & Compliance

New operating models impact risk postures and need to be re-assessed. Classify assets. Identify unmanaged controls, infrastructure, and software. Review workforce controls to ensure adherence to regulatory compliance requirements.

Identity & Access

MFA should be implemented for all remote workers who access corporate resources. Not all MFA types are created equal. Deploy privileged-access controls at remote workstations. Consider identity governance administration tools.

Endpoint Protection

Endpoint visibility and hardening is essential, as is application protection and data encryption. Controls and access for unmanaged devices.

Cloud Controls

Ensure cloud security controls are appropriate for the applications (including email), data, and access requirements of your business. Review and manage logs.

Physical Controls

Security training for a remote workforce should be considered.

Remote Access & Network Controls

In-depth assessment recommended. Massive growth in concurrent VPN connections impact performance. RDP can be risky. VPN infrastructure can be impacted by vulnerabilities and DOS attacks. Ensure proper segmentation and traffic analysis.

Monitoring, Alerting & Management

Organizations should consider using managed security services to monitor event logs for security incidents

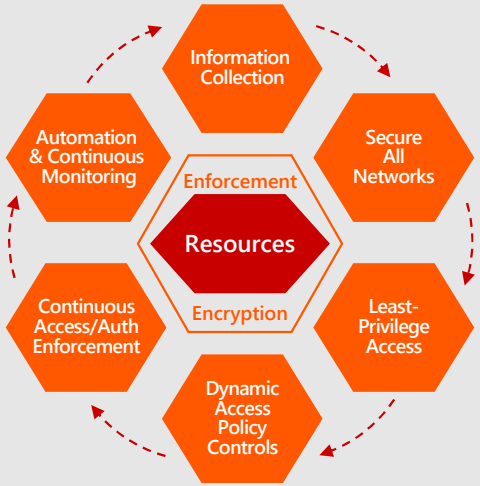
avanade Microsoft

Security Governance Frameworks already embrace ZT tenets, **but many organizations don't enforce them**

Problems with Legacy:

- Inconsistent governance models
- Added complexity and cost from sub-optimal designs and solutions
- Poor performance and user experience resulting from complex architectures and application performance
- Limited ability to meet changing business needs due to slow, inefficient architectures
- Create barriers to timely and efficient compliance audits
- Higher risk of data breach

Zero Trust Model



Organization Outcomes:

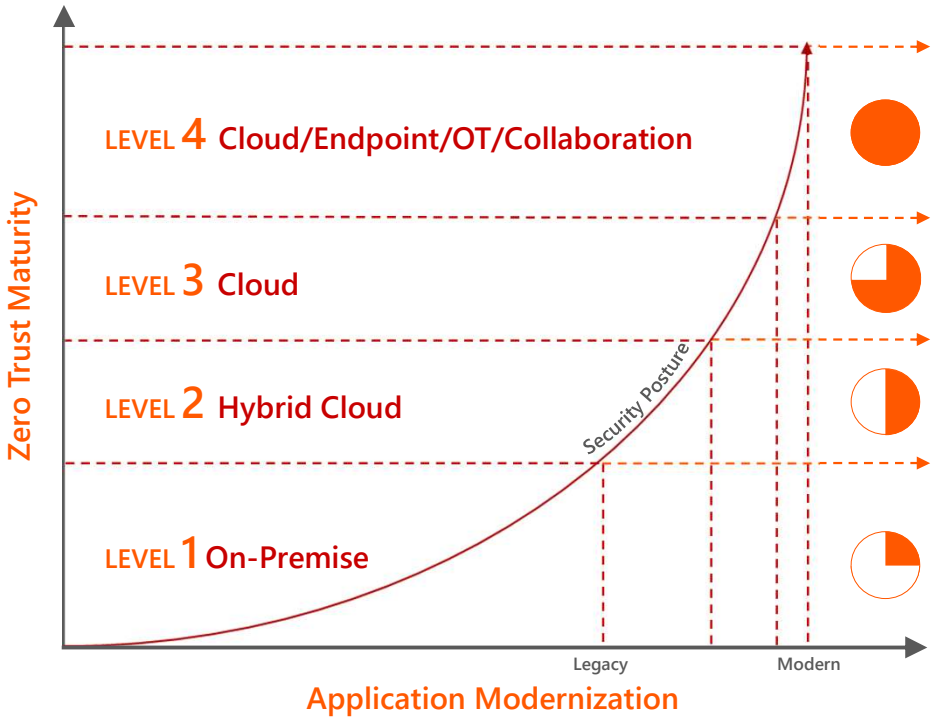
- Improve security posture with up to 90% reduction in successful attacks
- Reduce cost and complexity by phasing out targeted legacy systems
- Improve employee- and customer-experience
- 2-3X faster time-to-value for M&A integration
- Easier to achieve and demonstrate compliance

Types of threats mitigated by Zero Trust

- Opportunistic Attackers
- Targeted Attackers
- Insider Threats
- Trusted Insider
- State-Sponsored Actors

avanade Microsoft

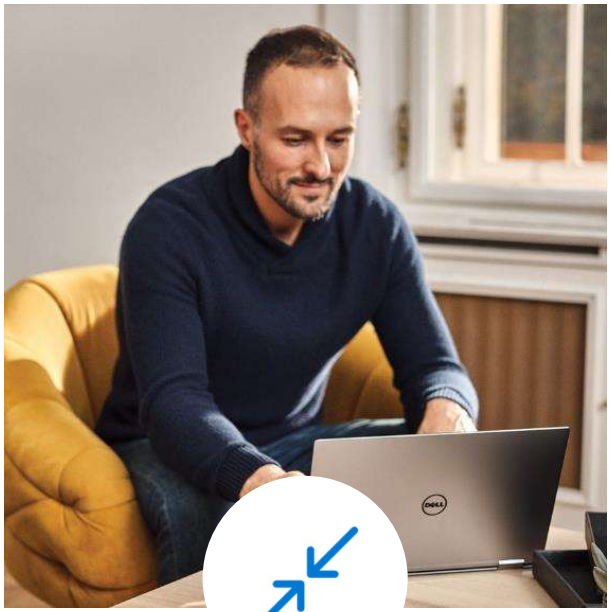
Accelerating security maturity and Zero Trust **through Cloud services & platform adoption**



avanade Microsoft

A new reality needs new principles

Verify explicitly



Use least privilege access

Assume breach

avanade Microsoft

Zero Trust across the digital estate

Identity | Devices | Apps | Infrastructure | Networking | Data

An integrated approach to securing access with adaptive controls and continuous verification across your entire digital estate

avanade Microsoft

Identities

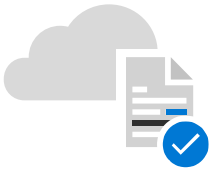
Zero Trust Objective: Verify and secure every identity with strong authentication

avanade Microsoft

Verify and secure every identity **with strong authentication**

Connect all of your users and applications

Verify identities with Multi-factor authentication (MFA)



Control access with smart policies and risk assessments

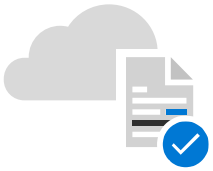
Enforce least privilege access with strong governance

avanade Microsoft

Verify and secure every identity **with strong authentication**

Connect all of your users and applications

Verify identities with Multi-factor authentication (MFA)



Control access with smart policies and risk assessments

Enforce least privilege access with strong governance

avanade Microsoft

Customer Example #1:

Connect all of your users and applications

Azure AD Staged rollout gave us the tools to implement a well-planned cutover. Once we set up modern authentication and Conditional Access, we created a test environment and split our users into groups. We tested our implementation of Azure AD with small groups. We evaluated how each step affected users and made changes as we went. This process simplified testing for our IT administrators.

When we selected cloud authentication, we expected to reduce costs, improve high availability, and remove burdensome server management from our IT administrators. These goals were realized. One benefit that we didn't anticipate: it is now much easier to integrate Software as a Service (SaaS) apps. With over 20 apps now **Since moving to Azure AD we've accelerated app onboarding by 5X! A huge productivity gain.**

Moving forward, we are collaborating with Microsoft to move towards passworldess and eventually a Zero Trust model. These initiatives include:

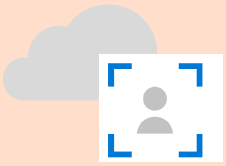
- **Password policy modernization**
- **Self-service password reset**
- **Passwordless implementation across the organization**

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/mitsui-said-goodbye-to-adfs-using-azure-ad-staged-rollout/ba-p/827851

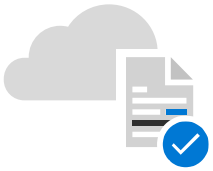
avanade Microsoft

Verify and secure every identity **with strong authentication**

Connect all of your users and applications



Verify identities with Multi-factor authentication (MFA)



Control access with smart policies and risk assessments

Enforce least privilege access with strong governance

avanade Microsoft

Customer Example #2:

Situation

- Client enforcing **password rotation**, thinking they were following best practice
- Lack of **cyber awareness** enabled attackers to succeed with phishing
- No **MFA** was established at acquired company
- Hacker **stole credentials**, created a spoofed O365 account, and redirected $750k offshore

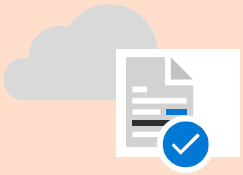
Avanade Solution

- Conducted a root-cause, and scope-of-damage assessment
- Shut down access to assets in fake O365 environment
- Implemented changes across entire organization: MFA, Conditional Access, Password Complexity, Legacy Auth Blocked, Tenant hardening, and Logging
- Recommended governance framework adherence process
- Revamped design documentation, and SOPs
- Rebuilt domain controllers

Verify and secure every identity **with strong authentication**

Connect all of your users and applications

Verify identities with Multi-factor authentication (MFA)



Control access with smart policies and risk assessments

Enforce least privilege access with strong governance

avanade Microsoft

Customer Example #3:

Control access with smart policies and risk assessments

With authentication for our apps handled by Azure AD, we can put in place the right security controls. Our security strategy is driven by a Zero Trust model. We don't automatically trust anything that tries to access the network. As we move workloads to the cloud and enable remote work, it's important to verify the identity of devices, users and services that try to connect to our resources.

To protect our identities, we've enabled a conditional access policy in conjunction with multi-factor authentication (MFA). When users are inside the network on a domain-joined device or connected via VPN, they can access with just a password. Anybody outside the networks must use MFA to gain access. We are also using Azure AD Privileged Identity Management to protect global administrators. With Privileged Identity Manager, users who want to access sensitive resources sign in using a different set of credentials from the ones they use for routine work. This makes it less likely that those credentials will be compromised.

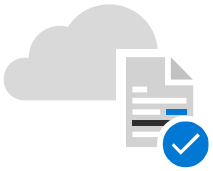
With Azure AD, we also benefit from Microsoft's scale and availability. Before we migrated our apps from the WAM to Azure AD, there were frequently problems with access related to the WAM. With Azure AD we no longer worry about downtime. Remote work is easier for employees, and we feel more secure.

- https://techcommunity.microsoft.com/t5/azure-active-directory-identity/johnson-controls-simplifies-remote-access-to-legacy-on-prem-apps/ba-p/1257351
- https://techcommunity.microsoft.com/t5/azure-active-directory-identity/johnson-controls-makes-working-from-home-easier-and-more-secure/ba-p/1257348

Verify and secure every identity **with strong authentication**

Connect all of your users and applications

Verify identities with Multi-factor authentication (MFA)



Control access with smart policies and risk assessments

Enforce least privilege access with strong governance

avanade Microsoft

Customer Example #4:

SIEMENS

"Whipping Zero Trust into the culture of a global technology company"

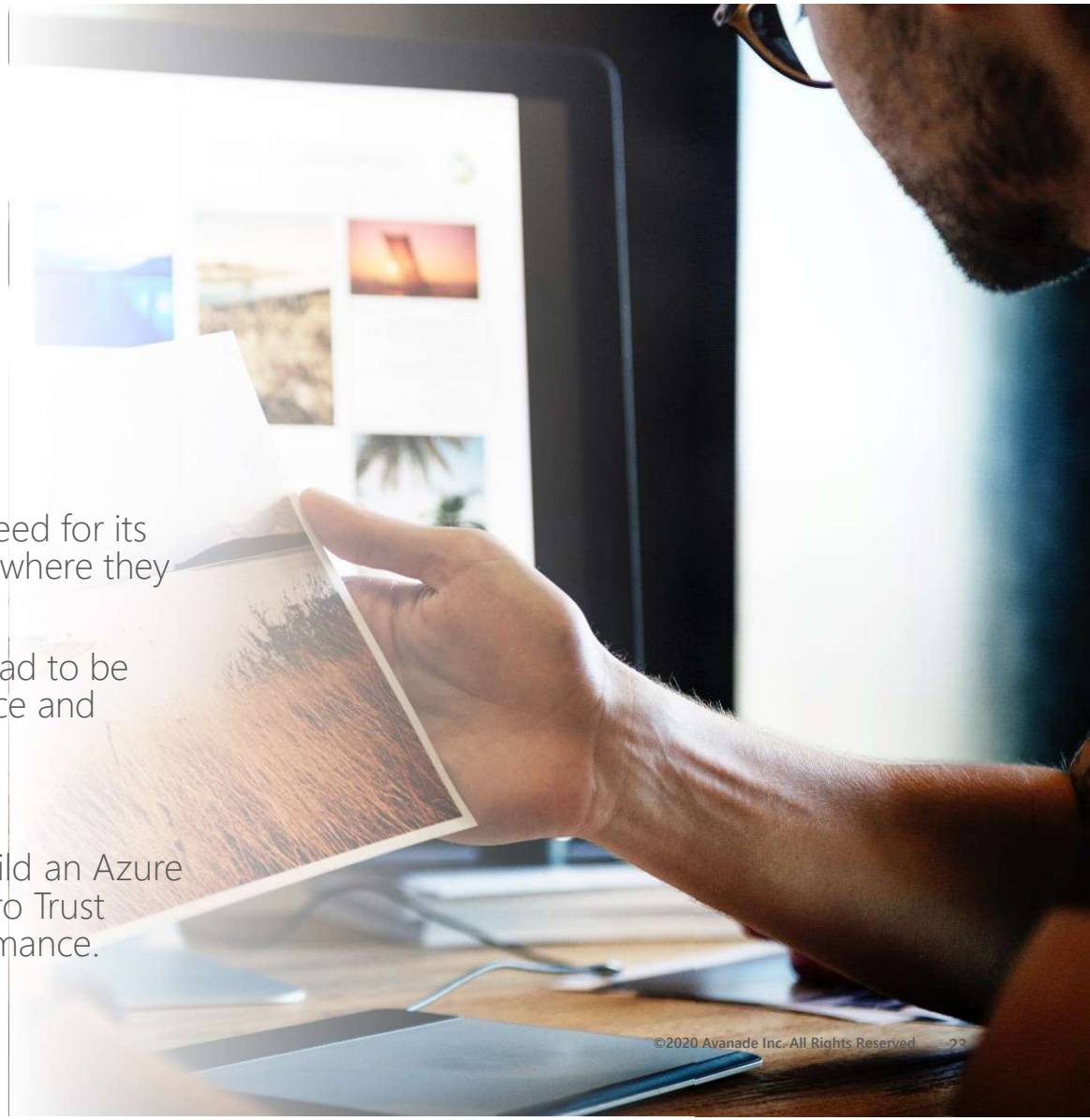
This 170-year-old firm has always recognized the need for its employees to have maximum flexibility in how and where they work.

As they planned to move to the cloud, Zero Trust had to be baked in, but not at the cost of employee experience and productivity.

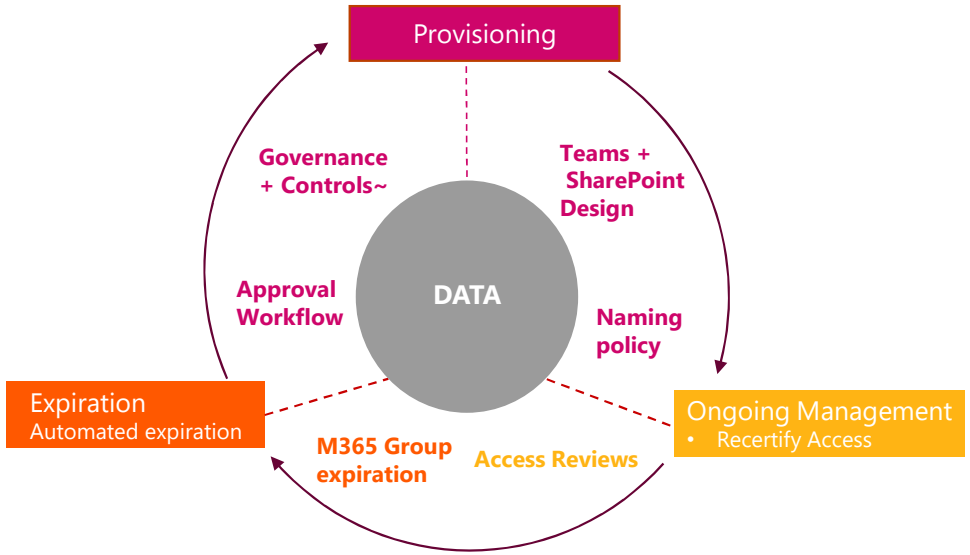
Avanade Solution

Avanade worked closely with their leadership to build an Azure AD-based identity platform that fully embraced Zero Trust concepts while maintaining core values and performance.

avanade Microsoft



Beginning The Journey - The Avanade Approach



avanade

Available resources

- **aka.ms/Zero-Trust**
- **avanade.com/security**
- **https://aka.ms/NISTZeroTrust**

Thank you for joining!

avanade